



1 JUN 21 32

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Paul C. Kocher, Joshua M. Jaffe,  
and Benjamin C. Jun

Application No.: 10/005,105

Filing Date: December 3, 2001

Title: Differential Power Analysis Method and  
Apparatus

Confirmation No.: 1675

Group Art Unit: 2132

Examiner: Nobahar, Abdulhakim

Attorney Docket No.: 44424162-8721

INFORMATION DISCLOSURE  
STATEMENT

SONNENSCHEIN NATH & ROSENTHAL LLP  
Customer No. 26263

Commissioner for Patents  
P.O. Box 1450  
Arlington, VA 22313-1450

**CERTIFICATE OF MAILING**  
I hereby certify that this correspondence is being deposited  
with the United States Postal Service as First Class Mail in an  
envelope addressed to: Commissioner for Patents, P.O.  
Box 1450, Alexandria, VA 22313-1450 on the date given  
below.

11 June 07

date of signature

Michael L. Day Reg. No. 55,101

Sir:

Pursuant to the provisions of 37 CFR § 1.56 and §1.97-§1.98, Applicants hereby submit  
patents, publications or other information enclosed herewith and listed on the enclosed Substitute  
for Form 1449B/PTO of which they are aware, which they believe may be material to the  
examination of this application and in respect of which there may be a duty to disclose. This  
IDS is being filed before the receipt of a first Office Action and after the filing of a Request for  
Continued Examination under §1.114 that was submitted on March 26, 2007.

A list of the patents and publications is set forth on the attached Substitute for Form  
1449B/PTO. A copy of the items on Form Substitute 1449B/PTO is supplied herewith.

While the information and references disclosed in this Information Disclosure Statement may be "material" pursuant to 37 CFR § 1.56, submission of this IDS is not intended to constitute an admission that any patent, publication or other information referred to herein is "prior art" for this invention unless specifically designated as such.

In accordance with 37 CFR § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 CFR § 1.56(a) exists. It is submitted that this Information Disclosure Statement complies with 37 CFR § 1.98 and MPEP § 609, and the Examiner is respectfully requested to consider the listed references.

Applicants believe no fee is due. However, the Commissioner is hereby authorized to charge our Deposit Account No. 19-3140 for any fees required in connection with the filing of this Information Disclosure Statement. This sheet is being submitted in duplicate.

Respectfully submitted,



Michael L. Day  
Reg. No. 55,101  
Attorney of Record

date of signature: 11 June 07

SONNENSCHEIN NATH & ROSENTHAL LLP  
P.O. Box 061080  
Wacker Drive Station, Sears Tower  
Chicago, Illinois 60606-1080  
(415) 882-2402

cc: IP/T docket CH (w.Substitute Form 1449A/PTO)  
J. Yang (DPA-OMNI) ( " )  
E. Radlo (w/o enclosure)



Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number

Institute for form 1449B/PTO				<b>Complete if Known</b>	
				Application Number	10/005,105
				Filing Date	December 3, 2001
				First Named Inventor	Paul C. Kocher
				Group Art Unit	2132
				Examiner Name	Abdulhakim Nobahar
Sheet	1	of	1	Attorney Docket No.	44424162-8721
<b>OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS</b>					
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.			T <sup>2</sup>
	2R	HEVIA, Alejandro et al., "Strength of Two Data Encryption Standard Implementations under Timing Attacks", Lecture Notes in Computer Science 1380 - LATIN '98: Theoretical Informatics 3rd latin American Symposium, Campinas, Brazil, April 1998; pp. 192-205.			
	2S	KOCHER, Paul, "Differential Power Analysis", The Risks Digest, Vol. 19(80), ACM Committee on Computers and Public Policy, New York, June 10, 1998. <a href="http://catless.ncl.ac.uk/Risks/19.80.html">http://catless.ncl.ac.uk/Risks/19.80.html</a>			
Examiner Signature				Date Considered	

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. <sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kinds Codes of USPTO Patent Documents at [www.uspto.gov](http://www.uspto.gov) or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). <sup>4</sup> For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. <sup>5</sup> Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. <sup>6</sup> Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file ( and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.